Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer program embodied in a computer-readable medium for scanning a computer for observer programs, the computer program comprising:

observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data;

reading instructions that read memory of the computer to obtain memory data;

comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; and

outputting instructions that provide the results through a graphical user interface.

2. (Original) The computer program of claim 1 wherein the memory data includes startup commands.

3. (Original) The computer program of claim 1 wherein the memory data includes registry startup commands.

4. (Original) The computer program of claim 1 wherein the plurality of observer program characteristics includes observer import table data and wherein the comparing

instructions compare memory import table data from the memory data characteristics with the observer import table data to determine whether an observer program is present on the computer.

5. (Original) The computer program of claim 1 wherein the plurality of observer program characteristics includes observer export table data and wherein the comparing instructions compare memory export table data from the memory data characteristics with the observer export table data to determine whether an observer program is present on the computer.

6. (Original) The computer program of claim 1 wherein the plurality of observer program characteristics includes observer resource data and wherein the comparing instructions compare memory resource data from the memory data characteristics with the observer resource data to determine whether an observer program is present on the computer.

7. (Original) The computer program of claim 1 wherein the plurality of observer program characteristics includes observer file content data and wherein the comparing instructions compare memory file content data from the memory data characteristics with the observer file content data to determine whether an observer program is present on the computer.

8. (Original) The computer program of claim 7 wherein the comparing instructions compare the observer file content data with the memory file content data at an offset address.

9. (Original) The computer program of claim 7 wherein the comparing instructions compare the observer file content data with a span of the memory file content identified by an offset address.

10. (Original) The computer program of claim 1 wherein the plurality of observer program characteristics includes observer module loading data and wherein the comparing instructions compare memory module loading data from the memory data characteristics with the observer module loading data to determine whether an observer program is present on the computer.

11. (Original) The computer program of claim 1 wherein the plurality of observer program characteristics includes OS observing functions and wherein the comparing instructions compare memory functions from the memory data characteristics with the OS observing functions to determine whether an observer program is present on the computer.

12. (Original) The computer program of claim 1 wherein the memory data includes explorer extension data.

13. (Original) The computer program of claim 1 wherein the memory data includes file use information.

14. (Original) The computer program of claim 1 wherein the memory data includes process information.

15. (Original) The computer program of claim 1 wherein the memory data includes running process information.

16. (Original) The computer program of claim 1 wherein the memory data includes loaded modules information.

17. (Original) The computer program of claim 1 wherein the memory data includes driver data.

18. (Original) The computer program of claim 1 wherein the memory data includes kernel driver data.

19. (Original) The computer program of claim 1 wherein the computer program further comprises disabling instructions to disable the observer program if it is present on the computer, the disabling instructions implementing a method comprising:
entering a startup command to load a kill program before the observer program is started;
rebooting the computer;
starting the kill program by execution of the startup command; and
deleting an observer program startup command so that the observer program is not started.

20. (Original) The computer program of claim 19 wherein the method further comprises deleting observer program files.

21. (Currently Amended) A method embodied in a computer-readable medium for scanning a computer for observer programs, the method comprising:

using observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data;

reading memory of the computer to obtain memory data;

comparing the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;

generating results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; and

outputting the results through a graphical user interface.

22. (Withdrawn) A computer program for detecting an observer program on a computer system, the computer program comprising:

a generator that generates activity observed by an observer program;

a system monitor that monitors the computer system to detect logging of the generated activity;

threshold data that defines suspect system activity;

code that causes the generator to begin generating the generated activity and that uses the system monitor to monitor the computer system during the generated activity and, based on the threshold data, provides information of any suspect system activity.

23. (Withdrawn) The computer program of claim 22 wherein the generator is a hardware keystroke generator comprising:

a processor;

memory in electronic communication with the processor programmed with generation instructions to cause the processor to generate keystrokes;

a communication port in electronic communication with the processor for outputting the keystrokes to the computer system.

24. (Withdrawn) The computer program of claim 22 wherein the generator is a software keystroke generator.

25. (Withdrawn) The computer program of claim 22 wherein the generator is a software generator.

26. (Withdrawn) A hardware keystroke generator for use in countering a hardware keystroke logger used on a computer, the hardware keystroke generator comprising:

a processor;

memory in electronic communication with the processor programmed with generation instructions to cause the processor to generate keystrokes;

a communication port in electronic communication with the processor for outputting the keystrokes to the computer system, the communications port comprising a keyboard-type connector for connecting the hardware keystroke generator to the keyboard port of the computer.

27. (Withdrawn) The hardware keystroke generator of claim 26 wherein a keystroke generation rate of the generator is configurable by a user.

28. (Withdrawn) The hardware keystroke generator of claim 27 wherein the generator is configurable by the user to set pauses in the keystroke generation.

29. (Withdrawn) The hardware keystroke generator of claim 28 wherein the generator is configurable by the user to use a variable rate for generating keystrokes.

30. (Withdrawn) A ciphering program for use on a single computer system to counter an observer program logging keystrokes, the ciphering system comprising:

ciphering entry instructions that capture input keystrokes on the single computer system before the observer program and creates ciphered keystrokes from the input keystrokes whereby the observer program logs the ciphered keystrokes;

ciphering exit instructions that receive the ciphered keystrokes after the observer program observes the ciphered keystrokes and creates the input keystrokes from the ciphered keystrokes whereby a user sees the input keystrokes as they are input; and

control instructions for controlling the ciphering process.

31. (Withdrawn) The ciphering program of claim 30 wherein the ciphering entry instructions are implemented on a hardware ciphering component comprising:

a processor;

memory in electronic communication with the processor programmed with the ciphering entry instructions; and

a communication port in electronic communication with the processor for outputting the ciphered keystrokes to the computer system.

32. (Withdrawn) The ciphering program of claim 30 wherein the ciphering entry instructions are implemented through software on the computer system.

33. (Withdrawn) A computer program for searching on a computer network for network sniffers, the computer program comprising:

sniffer data comprising a plurality of sniffer program characteristics descriptive of a plurality of the network sniffers where the network sniffers are programmed to observe network traffic on the computer network and to create log data including user identifications;

sending instructions that send response-requesting messages from the sniffer data across the computer network;

listening instructions that listen for network responses to the response-requesting messages;

comparing instructions that compare the plurality of sniffer program characteristics with the network responses to determine whether a network sniffer is present on the computer network;

generating instructions that generate results from the comparing, wherein the results generated indicate whether the network sniffer is present on the computer network; and

outputting instructions that provide the results through a graphical user interface.

34. (Withdrawn) A method for searching on a computer network for network sniffers, the method comprising:

using sniffer data comprising a plurality of sniffer program characteristics descriptive of a plurality of the network sniffers where the network sniffers are programmed to observe network traffic on the computer network and to create log data including user identifications;

sending response-requesting messages from the sniffer data across the computer network;

listening for network responses to the response-requesting messages;

comparing the plurality of sniffer program characteristics with the network responses to determine whether a network sniffer is present on the computer network;

generating results from the comparing, wherein the results generated indicate whether the network sniffer is present on the computer network; and

outputting the results through a graphical user interface.